EXORAPRIME

AML/KYC Policy

COMPANY	Exora Prime
REGISTRATION	2026-00044
EFFECTIVE DATE	April 07, 2026
VERSION	v1.0

Table of Contents

SECTION 01

Introduction and Regulatory Framework

1.1 Exora Prime, trading as Exora Prime Ltd (hereinafter referred to as "the Company"), is committed to the highest standards of Anti-Money Laundering ("AML") and Counter-Terrorist Financing ("CTF") compliance. This policy sets out the Company's procedures for preventing the use of its services for money laundering, terrorist financing, or other financial crimes.

1.2 This policy applies to all officers, employees, contractors, and agents of the Company. All personnel are required to familiarize themselves with this policy and to comply with its provisions in the performance of their duties.

1.3 The Company has appointed a designated Money Laundering Reporting Officer ("MLRO") who is responsible for overseeing the implementation of this policy, receiving internal suspicious activity reports, and filing external reports with the relevant authorities as required by law.

1.4 The Company's compliance department can be contacted at compliance@exoraprime.com for any questions or concerns relating to this policy.

SECTION 02

Definitions

Money Laundering

The process by which criminals attempt to conceal the true origin, ownership, or destination of illegally obtained funds by channelling them through legitimate financial systems or commercial activities.

Terrorist Financing

The provision, collection, or management of funds with the intention or knowledge that such funds will be used to carry out terrorist acts or to support terrorist organizations.

Customer Due Diligence (CDD)

The process of identifying and verifying the identity of a customer, understanding the nature and purpose of the business relationship, and assessing the money laundering and terrorist financing risk associated with the customer.

Enhanced Due Diligence (EDD)

Additional verification measures applied to customers or transactions that present a higher risk of money laundering or terrorist financing.

Politically Exposed Person (PEP)

An individual who is or has been entrusted with a prominent public function, including heads of state, senior government officials, senior judicial or military officials, senior executives of state-owned corporations, and important political party officials, as well as their immediate family members and close associates.

Beneficial Owner

The natural person(s) who ultimately own or control a customer and/or the natural person on whose behalf a transaction or activity is being conducted, including any person exercising ultimate effective control over a legal entity or arrangement.

Suspicious Activity Report (SAR)

A report filed internally with the MLRO or externally with the relevant regulatory authority when there are reasonable grounds to suspect that a transaction or activity may be related to money laundering or terrorist financing.

2.1 The definitions set out above shall apply throughout this policy unless the context otherwise requires. Terms defined in applicable legislation shall have the meanings ascribed to them in such legislation.

SECTION 03

Customer Due Diligence (CDD)

3.1 The Company shall conduct Customer Due Diligence on all prospective clients before establishing a business relationship or carrying out any transaction. No trading account shall be activated until the CDD process has been satisfactorily completed.

3.2 The CDD process requires the collection and verification of the following information for individual (natural person) clients:

- Full legal name as it appears on an official government-issued identification document;
- Date of birth;
- Nationality and country of residence;
- Residential address (not a P.O. Box);
- Valid government-issued photo identification (passport, national identity card, or driving licence);
- Proof of residential address issued within the last three (3) months (utility bill, bank statement, or government correspondence);
- Source of funds and source of wealth information;
- Tax identification number, where applicable.

3.3 For corporate clients, the CDD process additionally requires:

- Certificate of incorporation or equivalent registration document;
- Memorandum and Articles of Association (or equivalent constitutional documents);
- Register of directors and shareholders;

- Identification and verification of all beneficial owners holding, directly or indirectly, ten percent (10%) or more of the shares or voting rights;
- Identification and verification of all authorized signatories;
- Board resolution or power of attorney authorizing the opening of the account;
- Audited financial statements, where available;
- Proof of registered address and principal place of business.

3.4 The Company reserves the right to request additional documentation or information at any time during the business relationship if it considers such information necessary to fulfil its AML/KYC obligations.

3.5 Where the Company is unable to complete the CDD process to its satisfaction, it shall not establish the business relationship, shall not carry out any transactions, and shall consider filing a Suspicious Activity Report with the relevant authority.

SECTION 04

Enhanced Due Diligence (EDD)

4.1 The Company shall apply Enhanced Due Diligence measures in circumstances where the risk of money laundering or terrorist financing is assessed as higher than normal. EDD shall be applied, at a minimum, in the following situations:

- The client is a Politically Exposed Person (PEP), a family member of a PEP, or a known close associate of a PEP;
- The client is resident in, or the transaction involves, a country or jurisdiction identified as high-risk by the FATF or by the Company's own risk assessment;
- The client's ownership structure is unusually complex or opaque, making it difficult to identify the beneficial owner;
- The transaction is unusually large, complex, or has no apparent economic or lawful purpose;
- There are grounds for suspicion that the client's funds are derived from criminal activity.

4.2 Enhanced Due Diligence measures may include, but are not limited to:

- Obtaining additional identification documents or information from independent and reliable sources;
- Conducting enhanced background checks using reputable third-party databases and screening services;
- Requiring a detailed explanation of the source of funds and source of wealth, supported by documentary evidence;
- Obtaining senior management approval before establishing or continuing the business relationship;
- Increasing the frequency and intensity of ongoing monitoring of the business relationship and transactions.

4.3 The Company shall document the rationale for applying EDD, the additional measures taken, and the outcome of those measures. All EDD records shall be retained in accordance with the Company's

record-keeping obligations.

4.4 Where the EDD process reveals information that gives rise to suspicion of money laundering or terrorist financing, the matter shall be escalated immediately to the MLRO for assessment and, if appropriate, the filing of a Suspicious Activity Report.

SECTION 05

Ongoing Monitoring

5.1 The Company shall conduct ongoing monitoring of all business relationships and transactions to ensure that they are consistent with the Company's knowledge of the client, the client's business profile, risk assessment, and source of funds.

5.2 Ongoing monitoring includes, but is not limited to:

- Scrutiny of transactions undertaken throughout the course of the business relationship to ensure that they are consistent with the client's known profile and expected trading patterns;
- Monitoring for transactions that are unusually large, complex, or inconsistent with the client's stated financial position;
- Periodic review and updating of client identification documents and CDD/EDD information;
- Automated transaction monitoring systems that flag potentially suspicious activity based on predefined rules and thresholds;
- Regular review of clients against updated sanctions lists, PEP databases, and adverse media sources.

5.3 The frequency and depth of ongoing monitoring shall be commensurate with the risk level assigned to the client. Higher-risk clients shall be subject to more frequent and intensive monitoring.

5.4 Any unusual or suspicious activity identified through ongoing monitoring shall be reported promptly to the MLRO for further investigation and determination of whether a Suspicious Activity Report should be filed.

SECTION 06

Suspicious Activity Reporting

LEGAL OBLIGATION

All employees have a legal obligation to report any knowledge or suspicion of money laundering or terrorist financing. Failure to report a suspicion may constitute a criminal offence. Tipping off a client that a report has been or may be filed is also a criminal offence.

6.1 Where any employee of the Company knows, suspects, or has reasonable grounds to suspect that a client or transaction is connected with money laundering or terrorist financing, they must immediately file an internal Suspicious Activity Report with the MLRO.

6.2 The internal SAR must include all relevant facts, the nature of the suspicion, and any supporting documentation. The reporting employee must not disclose to the client or any third party that a report has been or may be filed ("tipping off").

6.3 Upon receipt of an internal SAR, the MLRO shall assess the information provided and determine whether there are reasonable grounds to file an external report with the relevant Financial Intelligence Unit (FIU) or other competent authority. The MLRO shall make this determination as soon as practicable.

6.4 Where the MLRO determines that a report to the relevant authority is warranted, the report shall be filed promptly and in the manner prescribed by applicable law. The MLRO shall maintain a record of all internal and external SARs, including the rationale for any decision not to file an external report.

6.5 The Company may suspend, freeze, or close a client's account pending the outcome of an investigation, where it considers such action necessary to comply with its legal obligations or to protect the integrity of its operations.

SECTION 07

Record Keeping

7.1 The Company shall maintain comprehensive records of all CDD and EDD information, transaction data, internal and external SARs, and any other documentation obtained in the course of fulfilling its AML/KYC obligations.

7.2 All records shall be retained for a minimum period of five (5) years from the date the business relationship ends, or from the date the transaction is completed, whichever is later, unless a longer retention period is required by applicable law or regulation.

7.3 Records shall be stored securely and shall be readily accessible to the MLRO, the compliance department, and any competent regulatory or law enforcement authority upon lawful request.

7.4 The Company shall ensure that its record-keeping systems are adequate to reconstruct individual transactions, including the amounts, currencies, dates, account details, and parties involved, so as to provide an audit trail for any investigation or regulatory inquiry.

SECTION 08

Sanctions Screening

8.1 The Company shall screen all prospective and existing clients against applicable sanctions lists, including but not limited to lists maintained by the United Nations Security Council, the European Union, the United States Office of Foreign Assets Control (OFAC), Her Majesty's Treasury (HMT), and any other relevant national or supranational authority.

8.2 Sanctions screening shall be performed at the point of client onboarding, upon any change to client information, and on a periodic basis as determined by the Company's risk assessment. The Company shall also screen counterparties, beneficial owners, and connected parties.

8.3 Where a potential match is identified against a sanctions list, the Company shall immediately escalate the matter to the MLRO and compliance department for further investigation. No transactions shall be processed for the client until the matter has been resolved.

8.4 If a confirmed match is established, the Company shall take all necessary steps to comply with the applicable sanctions regime, which may include freezing the client's account and assets, declining to process transactions, terminating the business relationship, and reporting the matter to the relevant authority.

8.5 The Company shall maintain up-to-date sanctions screening tools and databases and shall ensure that its screening processes are commensurate with its risk profile and the jurisdictions in which it operates.

SECTION 09

Client Non-Compliance

WARNING

Providing false, misleading, or incomplete information during the verification process, or using the Company's services for money laundering, terrorist financing, or any other financial crime, is a serious offence that may result in account termination, fund freezing, and referral to law enforcement authorities.

9.1 Clients are required to provide accurate, complete, and up-to-date information during the account opening process and at any time the Company requests updated documentation. Failure to do so may result in the restriction or suspension of the Client's account until the required information is provided.

9.2 The Company shall take appropriate action against any Client who is found to have provided false, misleading, or incomplete information during the verification process, or who is found to be using the Company's services for the purpose of money laundering, terrorist financing, or any other financial crime. Such action may include:

- Immediate suspension or termination of the Client's account;
- Freezing of the Client's funds pending investigation;
- Reporting the matter to the relevant regulatory and law enforcement authorities;

- Pursuing civil remedies to recover any losses suffered by the Company.

9.3 Clients who refuse to provide requested identification documents, source of funds documentation, or other information required for verification purposes shall have their account functionality restricted. Withdrawal of funds may be withheld until the Company is satisfied that all regulatory requirements have been met.

9.4 This policy is subject to periodic review and may be updated to reflect changes in applicable laws, regulations, or the Company's risk assessment. Clients will be notified of any material changes via the Company's website or by email.

Document	AML/KYC Policy
Company	Exora Prime
Effective Date	April 07, 2026
Website	https://exoraprime.com
Compliance Contact	compliance@exoraprime.com